PRACTICAL: 1

AIM:

A security training institute is setting up a lab for ethical hacking workshops. The team must decide whether to use Kali Linux or Parrot Security OS, prioritizing ease of installation, hardware requirements, and post-installation configuration for beginner and intermediate students. Evaluate and install the most suitable penetration testing operating system for a security team by exploring the installation processes and user-friendliness of Kali Linux and Parrot Security OS.

THEORY:

Penetration Testing OS Overview: Kali Linux and Parrot Security OS are specialized Linux distributions for ethical hacking and penetration testing. Both come with a wide range of pre-installed security tools. Kali is more advanced, while Parrot offers a more beginner-friendly experience with privacy features.

Ease of Installation & Configuration: Kali Linux requires more manual configuration post-installation. Parrot OS is easier to set up and is optimized for lower-resource systems. Both distributions are used in cybersecurity training environments for hands-on experience.

Tools in Kali Linux

Nmap- A network scanning tool for discovering hosts, open ports, and services running on a network, commonly used for vulnerability assessment and network mapping.

Netcat- A versatile networking tool used for reading and writing data across network connections. Often used for creating reverse shells and testing network connections.

Fluxion- A tool for performing social engineering-based Wi-Fi attacks, including phishing attacks to capture WPA handshakes and crack Wi-Fi passwords.

Lynis- A security auditing tool that performs system scans to detect vulnerabilities and weaknesses in a system's configuration, offering recommendations for hardening.

Wireshark- A network protocol analyzer used to capture and analyze network traffic in real-time, helpful for detecting issues like packet sniffing and man-in-the-middle attacks.

Tools in Parrot Security OS

Tor & Anonsurf- Tor is used for anonymous browsing by routing traffic through multiple servers, while Anonsurf integrates Tor with Parrot OS to anonymize all network activity.

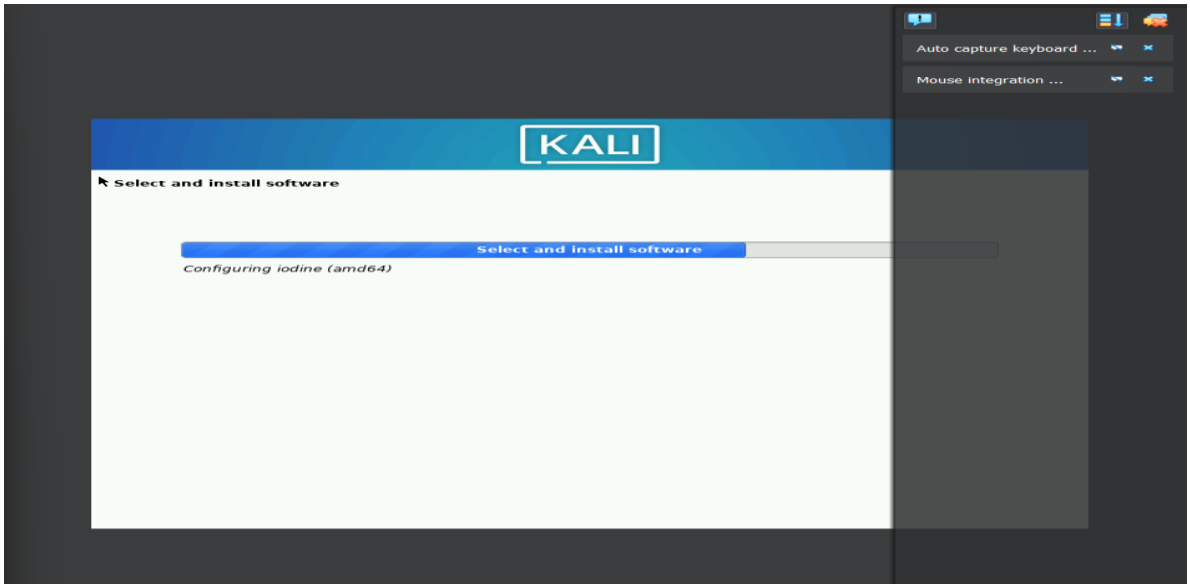
Electrum- A lightweight and secure Bitcoin wallet used for managing and transacting cryptocurrency with features like two-factor authentication and multi-signature support.

Kayak- A network monitoring tool that helps assess the security and performance of network traffic, similar to Wireshark, but with a lighter footprint and user-friendly interface.

EtherApe- A graphical network monitor that displays network activity in real-time. It visualizes connections and traffic flows between devices on a network.

Ricochet- A secure and anonymous instant messaging tool that uses the Tor network to allow users to communicate without revealing their location or identity.

OUTPUT:



LATEST APPLICATIONS:

Latest Applications of Kali Linux

Penetration Testing- Used to test networks, systems, and applications for vulnerabilities with pre-installed tools.

Red Teaming- Offensive teams use Kali for simulating attacks to assess security defenses.

Wireless Network Auditing- Tools like Aircrack-ng audit wireless networks for encryption weaknesses.

Web Application Security Testing- Tools like Burp Suite and OWASP ZAP identify web app vulnerabilities like SQL injection and XSS.

Social Engineering- Kali includes tools like Social-Engineer Toolkit (SET) for testing human vulnerabilities through phishing and other social engineering tactics.

Exploit Development- Kali provides environments and tools like Metasploit for creating and testing custom exploits on vulnerable systems.

Latest Applications of Parrot Security OS

Privacy and Anonymity- Tools like Tor and Anonsurf ensure anonymous browsing during testing.

Digital Forensics- Used for collecting and analyzing digital evidence in forensics investigations.

IoT Security Testing- Tools for testing the security of IoT devices and connected networks.

Secure Communications- PGP encryption and other tools ensure private communications during assessments.

Cryptography- Parrot offers tools for encryption and decryption, aiding in secure data handling and communication during tests.

Cloud Security- Parrot OS includes tools to test and secure cloud environments, identifying potential vulnerabilities in cloud infrastructure and services.

LEARNING OUTCOME:

From this practical, I gained hands-on experience with Kali Linux and Parrot OS. I learned how to install, configure, and use both operating systems, which helped me develop problem-solving skills and understand how to choose the right OS for different tasks.

REFERENCES:

1. Kali OS: https://www.kali.org/
2. Kali OS Installation: https://www.youtube.com/watch?v=jk2KGdJU2OI
3. Parrot Security OS: https://parrotlinux.org/
4. Parrot Security OS Installation: https://www.youtube.com/watch?v=4qvFp99rfXw
5. Kali Linux Tools: https://kali.org/tools/
6. Parrot Security Tools: https://linuxhint.com/parrot_os_tools_top_20/